



# Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 20 August 2003

Current Nationwide Threat Level is



[For info click here](#)

[www.whitehouse.gov/homeland](http://www.whitehouse.gov/homeland)

## Daily Overview

- The Associated Press reports investigators of the recent power outage are probing the role of the low-tech system of phones put in place to disseminate information between regional power groups to avert such a crisis. (See item [1](#))
- CBC News (British Columbia) reports thousands of people have been lined up at Vancouver International Airport, on Tuesday, as widespread computer problems have shut down Air Canada's check-in system. (See item [7](#))
- The Associated Press reports the Pima County Sheriff's Department and a federal law enforcement agency are investigating the theft of explosives from a University of Arizona laboratory located about 23 miles south of Tucson. (See item [26](#))
- Security Focus today raised ThreatCon to Level 3, with a subsequent need for increased vigilance.

### DHS/IAIP Update *Fast Jump*

Production Industries: [Energy](#); [Chemical](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [General](#); [DHS/IAIP Web Information](#)

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated**

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. *August 19, Associated Press* — Power grid warnings came late, if at all. Investigators of the Midwest and Northeast power outage are probing the role of the low-tech system of

**phones put in place to disseminate information between regional power groups to avert such a crisis.** Independent system operators across the country are tied together by a system of telephone hotlines. **The system was put in place after the 1965 blackout to provide individual operators with vital information about events occurring outside their jurisdictions.** Each system is so complex that operators are dependent on their counterparts to share information. Many phone lines are recorded. Those recordings, and logs of calls in and out of affected control rooms, will become key to the simultaneous investigations carried by industry groups, Congress and federal and state task forces. **The timing and content of the conversations preceding the blackout remain unclear, and the conversation between the Midwest and mid-Atlantic groups may have come seconds before the onset of the blackout.**

Source: [http://www.usatoday.com/news/nation/2003-08-19-blackout-warning\\_x.htm](http://www.usatoday.com/news/nation/2003-08-19-blackout-warning_x.htm)

2. *August 19, The Washington Post* — **Electricity council says it's too weak. The electric industry group that oversees the nation's power grid, born in an attempt to prevent disruptive blackouts, says it doesn't have the resources or authority to do that job in today's complex, deregulated market.** The voluntary system of standards under which utilities and the North American Electric Reliability Council (NERC) work is no longer adequate, according to NERC officials and many outside experts. For the past 35 years the Princeton, NJ-based NERC has been pressing generators, transmission-line companies and other companies in the industry to cooperate and to build in safety measures to deal with emergencies such as lightning strikes and fuel shortages. **Both houses of Congress have passed legislation including mandatory authority for NERC,** but the bills also cover much other ground and will be the subject of conference committee negotiations when Congress returns from its August recess.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A11626-2003Aug 18.html>

3. *August 19, The Associated Press* — **GAO probes FirstEnergy-owned nuke plant. The Government Accounting Office (GAO) is looking into the federal government's handling of problems at a nuclear plant owned by FirstEnergy – the Ohio-based utility at the center of the investigation into last week's blackout.** FirstEnergy's nuclear plant, shuttered since early last year, is the subject of an investigation by the Nuclear Regulatory Commission (NRC). The GAO, in turn, has been exploring the adequacy of NRC's inspection of the plant since late last year. **The investigative request from four members of Congress came after criticism of the NRC's handling of the Davis-Besse plant, located along western Lake Erie. It hasn't been operational since it went down for maintenance in February 2002, and month later, a leak was discovered where boric acid had eaten through much of a 6-inch-thick steel cap covering the plant's reactor vessel.** It was the most extensive corrosion ever at a U.S. nuclear reactor and led to a nationwide review of 69 other plants. The NRC has said the damage ranked at the agency's most serious level for safety problems. When the damage was discovered, FirstEnergy expected the plant to be closed for three months. But the startup date has been continually pushed back because of prolonged repairs throughout the plant.

Source: <http://www.washingtonpost.com/wp-dyn/articles/A13315-2003Aug 19.html>

4. *August 19, Dow Jones Business News* — **Unchecked ethnic strife in Niger Delta may hit oil output. Ongoing tribal fighting in the southern port city Warri will take "a heavy toll" on**

**onshore oil production if it escalates**, according to a Royal Dutch/Shell official. So far, five days' fighting between rival Ijaws and Itsekiris has been limited to the city, far from the oil rigs on the oil-rich Niger Delta or the offshore terminals. But the danger is that could change.

**Fighting between the rival ethnic groups last March forced multinational oil companies operating there to shut in about 800,000 b/d of crude oil, representing about 40% of Nigeria's OPEC quota then.** Warri has in recent years been in the grips of increasing ethnic and political violence, much of it over shares of the region's oil wealth. Nigeria is Africa's largest oil producer and the fifth-largest source of U.S. oil imports. Most of the oil is drilled in the southern Niger Delta.

Source: [http://biz.yahoo.com/djus/030819/1319001020\\_2.html](http://biz.yahoo.com/djus/030819/1319001020_2.html)

[\[Return to top\]](#)

## **Chemical Sector**

Nothing to report.

[\[Return to top\]](#)

## **Defense Industrial Base Sector**

5. *August 19, The Daily Herald (WA)* — **The 767-400ER is studied for another military role.** The 767-400ER will be a test-bed for the U.S. Air Force's E-10A program. **Instead of being filled with passengers, this 767 will be stuffed with electronics gear. Downward-looking radar and other sensors will keep track of military targets moving on the ground, while radios will maintain contact with U.S. warplanes.** Computers will integrate the two, so that target information collected by the surveillance plane flows quickly to attack pilots — or even unnamed aerial vehicles. **It's part of the military's move toward network-centered warfare, in which information moves from sensors to shooters more quickly.** The goal is to have as many as five E-10As deployed by 2013, according to an Air Force spokesman.

Source: <http://www.heraldnet.com/Stories/03/8/19/17360286.cfm>

[\[Return to top\]](#)

## **Banking and Finance Sector**

6. *August 19, Gulf Daily News (Bahrain)* — **Saudi go-ahead for anti-money laundering law.** On Monday, August 18, Saudi Arabia's government endorsed the kingdom's first ever anti-money laundering law which stipulates stiff penalties against offenders, as Riyadh stepped up its fight against terrorism. **The law requires financial institutions to keep records of transactions for a minimum of 10 years and adopt precautionary measures to uncover and foil money laundering operations.** It also requires banks and financial institutions to create Financial Intelligence Units to prepare reports on suspicious transactions to help minimize and detect such illegal operations. **The law allows exchange of information and judicial actions against money laundering operations with countries with which the kingdom maintains official agreements.** The twenty-nine article law stipulates jail terms of up to fifteen years and a fine of seven million riyals (USD\$1.86m) for those who carry out

money laundering through charities or organized gangs. The law also states that financing terrorism or terror organizations is an act punishable under the legislation provisions.

Source: <http://www.gulf-daily-news.com/Articles.asp?Article=59414&Sn=BUSI>

[[Return to top](#)]

## **Transportation Sector**

7. *August 19, CBC News (British Columbia)* — **More airport chaos for Air Canada passengers. Thousands of people have been lined up at Vancouver International Airport, on Tuesday, as widespread computer problems have shut down Air Canada's check-in system.** A virus has damaged the company's communications network, leaving passengers in a holding pattern. **Air Canada spokesperson Laura Cook says the airline's self-serve kiosks have been knocked out and counter computer check-in terminals have been slowed down. As a result, passengers are being checked in manually, and it's estimated it could take hours to clear the huge line-up.** Airport spokesperson Laurie Chambers acknowledges that some people may be uncomfortable outside in the hot sun. "We are bringing folks who require seats back into the building. We are handing out water." Earlier, passengers bound for Tokyo, Beijing and London were asked to leave the airport, and return early Tuesday afternoon. **Air Canada says the virus is affecting airlines all over the world, and that its technicians are installing a patch to combat the virus.** This is just the latest problem to slow travelers at the airport. Flights from Vancouver to the U.S. were delayed on Sunday by a security problem. Source: [http://vancouver.cbc.ca/regional/servlet/View?filename=bc\\_ai\\_rcan20030819](http://vancouver.cbc.ca/regional/servlet/View?filename=bc_ai_rcan20030819)
8. *August 19, East Bay Business Times* — **Oakland Airport gets security grant.** Officials of Oakland International Airport will receive a grant of more than \$11 million from the Federal Aviation Administration to upgrade their checked-baggage security screening system in Terminal Two. **That terminal houses gates used by Southwest Airlines, the airport's dominant carrier, accounting for 60 percent of its daily flights. The grant will help airport officials relocate the screening area from in front of the Southwest ticket counters to a new location behind the ticketing desks. That will give passengers waiting in line to check in for flights a lot more room.** "Moving the checked baggage security screening process will significantly reduce congestion in a facility that was designed to comfortably serve 3.5 million passengers per year," said Steven J. Grossman, director of aviation for the Port of Oakland, which operates the airport, in a prepared statement. "Southwest currently serves 60 percent of Oakland's passenger traffic or roughly about eight million passengers annually." **The grant will also help fund construction of facilities to house new Explosives Detection System (EDS) machines, allowing personnel for the Transportation Security Administration to screen more baggage for explosive devices with fewer workers.** Source: <http://eastbay.bizjournals.com/eastbay/stories/2003/08/18/daily8.html>
9. *August 19, Associated Press* — **Air Algeria hijacking foiled. A man attempted to hijack an Air Algeria jet Tuesday, threatening the crew with what he claimed was a grenade before surrendering to security services, Algeria's official news agency said.** The APS news agency said the hijacking attempt ended "without incident," but did not say how many passengers were on board or give information about injuries. The aircraft had taken off from the capital, Algiers, when the 55-year-old man threatened the crew with a box that he said

contained a grenade, APS reported. **The man, who was identified only by his first name, Brahim, demanded that the plane be diverted to the Swiss city of Geneva, according to the news agency. The crew of the Boeing 737, however, managed to convince him that the plane should land instead at the Algerian city of Oran, one of the flight's scheduled stops, to refuel and let passengers disembark, the agency said.** There, he surrendered to security services and the attempted hijacking ended "without incident," it reported. APS said he was mentally unstable. It was not clear from the report whether the man actually had a grenade. The news agency said the aircraft was on a flight from Algiers to Oran and was due to fly onward to the French city of Lille.

Source: <http://www.modbee.com/24hour/global/story/972578p-6824261c.html>

[\[Return to top\]](#)

## **Postal and Shipping Sector**

Nothing to report.

[\[Return to top\]](#)

## **Agriculture Sector**

**10. *August 19, National Science Foundation* — Genome sequence for tomato microbe. Scientists have sequenced the genome of the microbe that causes bacterial speck disease in tomato plants and have reported preliminary information about the roles of the more than 5,500 genes, including clues to how the bacterium infects plants that are constantly trying to defend themselves against pathogens.** The bacterium's host-infection mechanism is also similar to that used by many other plant, animal and human pathogens, including a number identified as priority targets for the nation's biodefense efforts. **The more than 50 strains of *P. syringae* infect a wide variety of crops worldwide.** "This model organism will give researchers a leg up on learning about pathogenesis for many other bacteria," said Jane Silverthorne, a program director at the National Science Foundation, which funded the project. Beyond the sequence of 6.5 million DNA base pairs, the team reports that the bacterium has nearly 300 genes related to virulence, more than 800 genes of unknown function not found in closely related bacteria, and a large number of so-called "mobile genetic elements." Mobile genetic elements permit the genome to change rapidly and may help *P. syringae* to interact with plants that evolve new ways to fend off infection.

Source: <http://www.sciencedaily.com/releases/2003/08/030819074507.htm>

**11. *August 19, Globe and Mail* — Cattle herd hits record on mad cow scare. The number of cattle on Canadian farms reached a record high in June after the discovery of a case of mad cow disease in Alberta resulted in the closure of the U.S. border to cattle and beef imports from this country, Statistics Canada said Tuesday. By the end of the month, the national herd of cattle and calves rose by 1.9 percent from the same month a year earlier. Most provinces, the agency said, have seen significant increases in herd sizes compared with the same period of 2002.** According to a survey of 25,000 farmers, livestock producers held a record 15.7 million of cattle on their farms as of July 1. The increase, Statistics Canada said, was "the result of limited foreign markets for Canadian cattle and beef." Following the

discovery of a single case of mad cow disease in Alberta in May, a number of countries shut their borders to imports from Canada. The United States, the destination for the bulk of Canadian beef exports, and Mexico have both since eased the restrictions.

Source: <http://www.globeandmail.com/servlet/story/RTGAM.20030819.wbcattleaug19/BNStory/Business/>

12. *August 18, Reuters* — Soybean aphid infestation hits U.S. soy states. Infestations of soybean aphids, pests that can sharply reduce crop yields, are being reported across the northern U.S. soy-growing states and leading agronomists and traders to expect lowered crop condition ratings on Monday. "There has been a lot of spraying for aphids during the past week," Dale Hicks, agronomist at University of Minnesota, said. "That increases the cost of production about 25 cents (per bushel). Spraying is costing them about \$10 an acre, and if they're averaging 40 bushels per acre." While it is known that aphids can sharply reduce soy yields, Hicks and other agronomists noted that data regarding yield-loss due to aphids was relatively sparse. **The soy pest had never been detected outside of Asia until July 2000, but in recent years has hit late-planted soybeans in the United States.** Aphids suck sap from the leaf's vascular system, resulting in plant stress and stunting. They additionally harm plants by transmitting viruses, agronomists said.

Source: [http://www.agriculture.com/default.sph/AgNews.class?FNC=goDetail\\_ANewsindex\\_html\\_50451\\_1](http://www.agriculture.com/default.sph/AgNews.class?FNC=goDetail_ANewsindex_html_50451_1)

[[Return to top](#)]

## **Food Sector**

Nothing to report.

[[Return to top](#)]

## **Water Sector**

13. *August 19, Associated Press* — Cleveland considers backup power for water pumps. Jane Campbell, mayor of Cleveland, OH, says the city will consider a backup electric power source to run water system pumps in the event of another blackout. The proposal outlined yesterday calls for linking city-owned Cleveland Public Power generators to pumping stations. All four pumping stations were knocked out by last Thursday's blackout, throughout parts of the northern United States and eastern Canada. The blackout cut water service to more than 1 million people.

Source: <http://www.onnnews.com/story.php?record=26134>

[[Return to top](#)]

## **Public Health Sector**

14. *August 19, Coloradoan* — Colorado city, county declare health emergency. West Nile virus cases are multiplying so fast that Larimer County, CO, has declared a public health emergency. The cities of Fort Collins and Loveland declared emergencies, and said they were



acting quickly to respond to a West Nile crisis. "The number of West Nile virus cases has been doubling every week and is expected to continue increasing as the peak of the season has not been reached yet," said Adrienne LeBailly, director of the county's health department. **The county had 137 West Nile cases, as of Monday.** Fort Collins City Manager John Fischbach has declared a local emergency and was working to finalize mosquito-spraying agreements. City officials have estimated that the entire battle plan could cost up to \$200,000. **The state has applied to the U.S. Centers for Disease Control and Prevention for \$4.5 million in grant money that would focus on mosquito-spraying operations.** The virus' spread through Larimer County is concentrated largely in Fort Collins and Loveland and areas within one mile of the cities.

Source: <http://www.coloradoan.com/news/stories/20030819/news/88481.html>

15. *August 19, Saint Louis University* — **New generation of smallpox vaccines to be tested. Two new investigational smallpox vaccines will be studied as part of a clinical trial starting soon at Saint Louis University's Center for Vaccine Development.** Saint Louis University is the only location in the U.S. participating in the trial. **The investigational vaccines will be compared with the existing smallpox vaccine, known as Dryvax. The new vaccines were produced using modern methods of cell cultivation.** Dryvax, the same smallpox vaccine that was provided to all U.S. residents during the period of routine smallpox vaccination, hasn't been produced in many years. The study will include 90 adult volunteers: 30 receive one newly produced smallpox vaccine, 30 receive the other new vaccine and 30 will receive Dryvax. "The effectiveness of these smallpox vaccines will be measured by observing whether or not a pock forms at the site of the vaccination, and through blood tests," said Sharon Frey, principal investigator for the study.

Source: [http://www.eurekalert.org/pub\\_releases/2003-08/slu-ngo081903.php](http://www.eurekalert.org/pub_releases/2003-08/slu-ngo081903.php)

16. *August 19, Associated Press* — **Early detection of outbreaks. The University of Nebraska and the nation's largest railroad are developing a system to track worker absences that could lead to early detection of disease outbreaks, including a bioterrorist attack.** "We want to find an outbreak of disease almost before it is happening," said Steven Hinrichs, head of the university's Center of Biosecurity. Union Pacific Corp. has used computers for years to track the availability of its train crews. It already knows to expect fewer workers at certain times, such as during deer hunting season, spokesman John Bromley said. **The railroad covers the western two-thirds of the country with at least 20,000 engineers and conductors constantly registering their availability for work, Bromley said.** Enough is known about trends on the railroad to detect unusual spikes in people staying home from work. **"Something different or wild would pop up right away," Bromley said. "If there as an episode of Asian flu or something we would see it almost immediately."** The university is seeking a federal grant to pursue development of the tracking system, which could be extended to other key industries, including airlines and electrical companies, Hinrichs said.

Source: <http://www.casperstartribune.net/articles/2003/08/19/news/coming/9c202e9e28264487b14dd06ed1a9352b.txt>

17. *August 18, Canadian Press* — **WHO sending specialist to Canada. The World Health Organization (WHO) has dispatched an expert to Canada to study a mysterious outbreak of respiratory illness in a British Columbia nursing home that appears to be caused by the virus responsible for Severe Acute Respiratory Syndrome (SARS).** WHO asked for and was

granted permission to send a specialist to the National Microbiology Laboratory in Winnipeg, said Paul Gully, Health Canada's pointman on SARS. **With no new cases reported in the world since June, WHO continues to hope SARS has been eradicated from the human population.** But it fully expects to be faced with frenzied reports of clusters of suspicious SARS-like respiratory ailments as the cold and influenza season for the Northern Hemisphere approaches in late fall and early winter. It hopes that by getting a better handle on what is going on at the Kinsman Place Lodge in Surrey it will be better prepared to handle "these hits," said Dick Thompson, director of communications for the WHO's communicable diseases branch.

Source: <http://canada.com/national/story.asp?id=B5103465-5456-4396-9851-C71AFB97E52D>

[[Return to top](#)]

## **Government Sector**

18. *August 19, Federal Computer Week* — **DHS to host alert system fair. Homeland Security Department officials plan to host an industry day in October for companies to show off their solutions for public warnings and alert systems. The event will help the new federal department decide what kind of systems work best,** said Rose Parkes, the acting chief information officer for the Federal Emergency Management Agency, which is now part of DHS. She said the event is in the planning stages with DHS's Science and Technology Directorate and Information Assurance office.

Source: <http://fcw.com/fcw/articles/2003/0818/web-dhs-08-19-03.asp>

19. *August 18, New York Times* — **Intelligence to be shared, Ridge tells governors. Tom Ridge, Secretary of the Department of Homeland Security, told the nation's governors today that his department was taking added steps to make sure they are given all necessary intelligence to respond quickly to a terrorist attack or the threat of one.** Speaking at the summer meeting of the National Governors Association, in Indianapolis, Ridge said that in addition to the governors, five senior officials in each state would be given top-secret security clearances to receive classified information, and that when the color-coded terror alert changed, governors would get any information federal intelligence agencies have on specific targets. **In public remarks to the state leaders — which echoed what he said to them in a private session earlier — Ridge outlined other steps that the Bush administration was taking to make the country's terror-response system more effective.** Among other things, he said the department was creating a "one-stop shop" that would make applying for federal grants easier and faster for governors.

Source: <http://www.nytimes.com/2003/08/19/politics/19GOVS.html>

[[Return to top](#)]

## **Emergency Services Sector**

20. *August 19, Government Technology* — **FCC issues wireless E911 call to action. FCC Chairman Michael Powell recently issued a "call to action" to state governors and state and local public safety officials to join the FCC in ensuring that emergency call centers**



**can identify the locations of people making 911 emergency calls from wireless phones.** In a speech before the Association of Public Safety Communication Officials (APCO) International Inc., Powell said, "We know that wireless enhanced 911 technology works — and can save lives." Powell said he had invited gubernatorial and tribal representatives to attend a meeting of the FCC's E911 Coordination Initiative on October 29–30 in Washington "to tackle current deployment issues, accuracy requirements and additional public education efforts." **Studies have shown that nearly a third of 911 calls today are from wireless phone users. The FCC's Phase I E911 rules required wireless carriers, within six months of a valid request from a public safety answering point — the 911 call center, to begin supplying to emergency dispatchers the telephone number of a wireless 911 caller and the location of the cell site or base station transmitting the call.**

Source: <http://www.govtech.net/news/news.php?id=2003.08.19-64604>

- 21. *August 19, Government Technology* — NIST developing virtual reality training tool for firefighters.** The National Institute of Standards and Technology (NIST) is developing a virtual reality simulation of fire situations that will enable fire professionals to demonstrate how life-threatening conditions can develop in structures and to test firefighting tactics on computers without risk to life and limb. **To build a realistic physics-based computer fire simulations, NIST experts are reworking the agency's fire modeling software — known as the Fire Dynamic Simulator (FDS) — and fire imaging program — known as Smokeview. Refinements to FDS will increase the system's ability for simulating the smoke, hot air and other gas flow caused by fire, wind, ventilation and structural conditions. The upgrade also will improve data processing, yielding speedier calculations that will permit even the most complex fires (such as a multistory or multibuilding event) to be portrayed.** NIST will be working with firefighter instructors to develop a simulation of all possible outcomes for different fire scenarios used in training. These will be incorporated into a software package, enabling users to change a simulation with the click of a mouse.

Source: <http://www.govtech.net/news/news.php?id=2003.08.19-64605>

- 22. *August 19, New York Times* — Disaster plans get new scrutiny after blackout.** After last week's power failure that blanketed an area stretching from the Northeast to the Midwest, companies are taking a harder look at whether their disaster recovery plans go far enough — literally. "The geographic dispersion of this event really causes some rethinking for companies," said Jim Simmons, the chief executive of a company that runs disaster recovery centers for about 10,000 clients in North America and Europe. **Having operations distributed across the nation is an old and honored strategy for companies with big call centers,** said Gary Morgenstern, a spokesman for AT&T. When a call center in New York goes down, he said, "that traffic is automatically routed to the West Coast," and the flow of commerce continues. **Government regulations of financial industries, meanwhile, increasingly require substantial efforts aimed at ensuring stability in an emergency.**

Source: <http://www.nytimes.com/2003/08/19/technology/19BACK.html?th>

- 23. *August 18, Associated Press* — Crowded airways interfere with emergency radio frequencies.** The Washington, DC region seems to be taking note of growing interference nationwide with emergency radio frequencies used by police and firefighters. The Washington Post reports booming mobile phone use is crowding airwaves and causing the problem from wireless company signals. A Fairfax County spokeswoman says initial

interference problems with the county's radio system were solved after some wireless companies reconfigured their systems. A spokesman for Montgomery County says its communication system is on a different part of the spectrum than local wireless phone networks, making it less prone to problems. **The Post reports DC plans to build seven transmitters and receivers to increase its radio system's signal. It filed an interference complaint last spring and has been given a \$40 million dollar federal grant.**

Source: [http://www.wusatv9.com/news/news\\_article.asp?storyid=21713](http://www.wusatv9.com/news/news_article.asp?storyid=21713)

[\[Return to top\]](#)

## **Information and Telecommunications Sector**

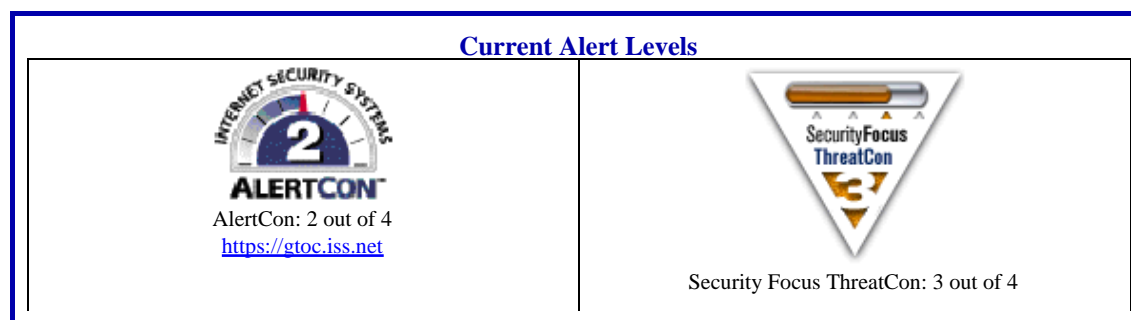
**24. *August 19, Associated Press* — New worm snarls computers at aerospace giant Lockheed Martin.** A new computer that exploits Microsoft's Windows operating system forced aerospace giant Lockheed Martin to shut down parts of its nationwide computer network this week, officials say. The worm follows the so-called "Blaster" or "LoveSan" worm that infected hundreds of thousands of computers worldwide last week. **For Lockheed Martin, the new worm caused the most trouble in Valley Forge, PA, and across the Denver area, where it infected 1,200 company computers.** Officials say the latest worm targeted computers that hadn't received a patch against last week's worm. **Lockheed Martin employees were unable to retrieve e-mail or get on the network** as a result. A downloadable software "patch" to fix the problem exploited by the worm had been available July 16, and Microsoft delivered it to home computer users who have the "automatic updates" feature enabled. However, the feature isn't geared for complex corporate computing systems, and many patches or other suggested solutions have to be carefully tested to see if they contain flaws.

Source: <http://www.fortwayne.com/mld/newssentinel/6568352.htm>

**25. *August 19, Federal Computer Week* — Navy Marine Corps Intranet goes down. A virus took the Navy Marine Corps Intranet (NMCI) off-line Tuesday, August 19.** A phone recording on the NMCI Strike Force hotline stated: "We are currently experiencing connectivity issues enterprise wide to include e-mail, Web and shared drive access due to a virus." NMCI is an enterprisewide network designed to connect everyone in the Navy and Marine Corps on a single, secure network. Since users started being moved to the system in 2001, almost 97,000 seats have been shifted from legacy systems.

Source: <http://www.fcw.com/fcw/articles/2003/0818/web-nmci-08-19-03.asp>

### **Internet Alert Dashboard**



		<a href="http://analyzer.securityfocus.com/">http://analyzer.securityfocus.com/</a>
<b>Current Virus and Port Attacks</b>		
<b>Virus:</b>	#1 Virus in the United States: <b>WORM_LOVGATE.G</b> Source: <a href="http://wtc.trendmicro.com/wtc/wmap.html">http://wtc.trendmicro.com/wtc/wmap.html</a> , Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]	
<b>Top 10 Target Ports</b>	135 (epmap), 137 (netbios-ns), 80 (www), 445 (microsoft-ds), 1434 (ms-sql-m), 1433 (ms-sql-s), 21 (ftp), 593 (http-rpc-epmap), 139 (netbios-ssn), 17300 (Kuang2TheVirus) Source: <a href="http://isc.incidents.org/top10.html">http://isc.incidents.org/top10.html</a> ; Internet Storm Center	

[\[Return to top\]](#)

## **General Sector**

**26. *August 19, Associated Press* — Authorities investigating explosives theft at University of Arizona lab. Members of the Pima County Sheriff's Department and a federal law enforcement agency are investigating the theft of explosives from a University of Arizona laboratory that is located about 23 miles south of Tucson, AZ.** The stolen material includes 34 sticks and 11 large tubes of dynamite as well as a chemical primer. The items were clearly marked as explosive and were stolen from the university's San Xavier Mining Laboratory near Sahuarita, AZ, between August 7 and August 14. The lab is used for teaching and research by mining and geological engineering students.

Source: [http://www.kvoa.com/stories/8/8192003\\_1.html](http://www.kvoa.com/stories/8/8192003_1.html)

**27. *August 19, CNN* — United Nations chief killed in Baghdad explosion.** A bomb explosion ripped through the United Nation's headquarters in Baghdad, Tuesday, August 19. **Sergio Vieira de Mello, the organization's special representative in Iraq, was among the 17 killed and 100 injured when a truck bomb exploded immediately beneath the window of his office in the Canal Hotel.** The building was evacuated as flames and smoke rose from the wreckage and windows reportedly were shattered as far as a kilometer away. **The bombing continues a recent pattern of attacks on non-military targets in Iraq. Over the weekend, oil, water and electricity lines were attacked by what a coalition spokesman called saboteurs.** And earlier this month, a car bomb exploded outside the Jordanian Embassy in Baghdad, leaving 10 people dead.

Source: <http://www.cnn.com/2003/WORLD/meast/08/19/sprj.iqr.main/inde x.html>

**28. *August 19, Associated Press* — Suicide bomber attacks Jerusalem bus. A suicide bomber blew himself up Tuesday, August 19, on a packed bus on a main thoroughfare in Jerusalem, killing at least 20 people and wounding 80, authorities said.** The bombing threatened to restart the cycle of attacks and retaliation that could derail a U.S.-backed "road map" peace plan to Palestinian statehood. In Washington, the White House deplored the bombing and offered sympathies to the victims and their families. **"We condemn this vicious act of terrorism," said Sean McCormack, a spokesman on national security issues. "We call on the Palestinian Authority to dismantle terrorism."** Over the weekend, Israel and the Palestinians had reached agreement on the handover of four West Bank towns to Palestinian

control.

Source: <http://www.washingtonpost.com/ac2/wp-dyn/A15067-2003Aug19?language=printer>

[\[Return to top\]](#)

## **DHS/IAIP Products & Contact Information**

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web-site (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

[DHS/IAIP Warnings](#) – DHS/IAIP Assessments, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

[DHS/IAIP Publications](#) – DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

[DHS/IAIP Daily Reports Archive](#) – Access past DHS/IAIP Daily Open Source Infrastructure Reports

### **DHS/IAIP Daily Open Source Infrastructure Report Contact Information**

Content and Suggestions: [nipcdailyadmin@mail.nipc.osis.gov](mailto:nipcdailyadmin@mail.nipc.osis.gov) or contact the DHS/IAIP Daily Report Team at 703-883-6631

Subscription and Distribution Information: Send mail to [nipcdailyadmin@mail.nipc.osis.gov](mailto:nipcdailyadmin@mail.nipc.osis.gov) or contact the DHS/IAIP Daily Report Team at 703-883-6631 for more information.

### **Contact DHS/IAIP**

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at [nipc.watch@fbi.gov](mailto:nipc.watch@fbi.gov) or call 202-323-3204.

### **DHS/IAIP Disclaimer**

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.